대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0002965
Application Number

출 원 년 월 일 : 2003년 01월 16일
Date of Application JAN 16, 2003

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2003 년 09 월 24 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0011
【제출일자】	2003.01.16
【국제특허분류】	H04L
【발명의 명칭】	암호화 장치 및 암호화 방법
【발명의 영문명칭】	Data Encryption apparatus and method
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	이영필
【대리인코드】	9-1998-000334-6
【포괄위임등록번호】	1999-009556-9
【대리인】	
【성명】	이해영
【대리인코드】	9-1999-000227-4
【포괄위임등록번호】	2000-002816-9
【발명자】	
【성명의 국문표기】	최양림
【성명의 영문표기】	CHOI,Yang Lim
【주민등록번호】	710120-1830615
【우편번호】	463-060
【주소】	경기도 성남시 분당구 이매동 124 한신아파트 210동 1509호
【국적】	KR
【발명자】	
【성명의 국문표기】	최윤호
【성명의 영문표기】	CHOI,Yun Ho
【주민등록번호】	730121-1480318

【우편번호】	138-222
【주소】	서울특별시 송파구 잠실2동 주공아파트 259동 407호
【국적】	KR
【취지】	특허법 제42조의 규정에 의하여 위와 같이 출원합니다. 대리인 이영필 (인) 대리인 이해영 (인)
【수수료】	
【기본출원료】	20 면 29,000 원
【가산출원료】	8 면 8,000 원
【우선권주장료】	0 건 0 원
【심사청구료】	0 항 0 원
【합계】	37,000 원
【첨부서류】	1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 오디오 비디오(A/V) 스트림의 암호화 기술에 관한 것으로, 구체적으로는 오디오 비디오 스트림의 암호화 장치 및 방법, 오디오 비디오 스트림의 암호화 시에 사용되는 암호화 키(encryption key)의 생성시에 필요한 난수(random number)를 생성하는 장치 및 방법에 관한 것이다. 본 발명의 암호화 장치는 오디오 비디오 스트림을 입력받아 소정의 처리를 수행하고, 난수 생성에 사용되는 소정의 데이터를 생성하여 출력하는 콘텐트 처리부; 상기 콘텐트 처리부로부터 상기 소정의 데이터를 입력받아 난수를 생성하는 난수 생성부; 상기 난수를 포함하는 정보를 입력받아 암호화키를 생성하는 암호화키 생성부; 및 상기 암호화키를 사용하여 상기 콘텐트 처리부에서 출력된 오디오 비디오 스트림을 암호화하는 콘텐트 암호화부를 구비한다. 본 발명에서 제시한 방법을 사용하여 생성된 난수는 비디오 데이터의 통계적 특성을 이용하여 생성되었기 때문에 랜덤 특성(randomness)이 좋은 효과가 있다.

【대표도】

도 3

【명세서】

【발명의 명칭】

암호화 장치 및 암호화 방법{Data Encryption apparatus and method}

【도면의 간단한 설명】

도 1은 오디오 비디오 스트림을 암호화하여 출력하는 장치의 블록도이다.

도 2는 LFSR을 사용한 난수 생성방법을 설명하기 위한 도면이다.

도 3은 본 발명의 오디오 비디오 스트림 암호화 장치의 블록도이다.

도 4는 본 발명의 오디오 비디오 스트림 암호화 방법의 플로우차트이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<5> 본 발명은 오디오 비디오(A/V) 스트림의 암호화 기술에 관한 것으로, 구체적으로는 오디오 비디오 스트림의 암호화 장치 및 방법, 오디오 비디오 스트림의 암호화 시에 사용되는 암호화 키(encryption key)의 생성시에 필요한 난수(random number)를 생성하는 장치 및 방법에 관한 것이다.

<6> 암호 시스템은 암호화 키의 관리 형태에 따라 대칭키(또는 비밀키라고도 함)암호 시스템과 비대칭키(또는 공개키라고도 함) 암호 시스템으로 구분된다. 대칭키 암호 시스템은 공개키 암호 시스템이 나오기 전에 주로 사용되던 암호 방식으로, 암호화와 복호화에 동일한 키를 사용하는 방식이다. 예를 들면, 송신자는 전송하고자 하는 평문 메시지를 암호화 키와 암호 알고

리즘을 통해 암호문으로 변환시켜 수신자에게 전송하면, 수신자는 동일한 키를 복호 알고리즘에 사용해서 원래의 평문으로 만든다.

<7> 이때 수신자는 암호화 통신을 하기 전에 안전하게 키를 교환하여야 하며, 암호 통신을 도청하려는 제3자는 송신자와 수신자가 사용한 키가 없으면 원래의 평 문을 알 수 없다. 그러나, 키 관리의 문제와 암호화 하고자 하는 상대방이 많으면 그에 따라 관리해야 하는 키의 수도 증가하게 되므로 키 관리 및 교환에 문제가 생긴다.

<8> 이에 비하여 비대칭키 암호화 시스템은 수학적 함수를 기반으로 하며, 대칭키 암호 시스템과 달리 한 쌍의 키가 존재하여 하나의 키는 누구든지 사용할 수 있도록 공개하고 다른 하나는 자신만이 비밀스럽게 보관하는 방식이다. 이때, 공개하는 키를 공개키(public key)라고 하며 비밀스럽게 보관하는 키를 개인키(private key)라고 한다.

<9> 공개키를 이용해서 송신자와 수신자가 암호 통신을 하기 위해서, 먼저 송신자는 수신자의 공개키로 메시지를 암호화하여 전송하고, 수신자는 자신의 개인키로 암호문을 복호화 하여 평문을 얻는다. 네트워크 상에서 누군가 암호문을 얻더라도 개인키 없이는 암호문을 복호화할 수 없으므로 안전하게 데이터를 전송할 수 있다. 왜냐하면, 개인키는 언제나 소유자만이 보관하고 있으며, 전송되거나 다른 사람에게 알려질 필요가 없기 때문이다

<10> 대칭키(symmetric cipher)는 브로드캐스트된 스트림을 암호화/복호화 (encryption/decryption) 하는데 많이 사용된다. 왜냐하면 대칭키를

사용한 암호화/복호화는 매우 빠르게 수행될 수 있고, 대칭키는 제한적 사용자에 대한 인증을 거친 사용자만이 접근할 수 있는 제한적 액세스 시스템을 통해서 안전하게 전송될 수 있기 때문이다. 일단 오디오 비디오 스트림이 셋톱박스(set-top box)나 PVR(Personal Video Recoder)에 입력되고 그 입력된 오디오 비디오 스트림을 나중에 사용하기 위하여 저장할 필요가 있는 경우에, 수신기(receiver)는 입력된 오디오 비디오 스트림을 암호화(encryption)할 필요가 있다. 왜냐하면 저작권(copyright)을 보호하고, 콘텐트의 복사를 관리할 필요가 있기 때문이다.

<11> 따라서 저장장소를 가지고 있는 수신기는 이와 같이 암호화 및 복호화를 수행할 암호화 복호화 엔진을 갖추고 있어야 한다. 암호화 및 복호화 수행시에 AES(Advanced Encryption Standard)나 TripleDES(Triple Data Encryption Standard) 가 가장 많이 사용된다.

<12> DES 는 "Data Encryption Algorithm(DEA)라는 표준으로 ANSI3.92에 의해 첫번째로 승인된 세계적인 표준 블록 암호기(block cipher)인데, 현재는 FIPS PUB 46-3에 "Data Encyption Standard(DES)"라는 표준으로 제정되어 있다. TripleDES 는 DES 암호기(cipher)의 3배수(3중) 버전으로, EDE(encrypt- decrypt - encrypt) 모드에서 2개의 키가 블록을 3번 암호화하는데 사용되기 때문에 DESede로 불리기도 한다.

<13> AES(Advanced Encryption Standard)는 미국의 암호관련 업계가 제출한 차세대 국가 암호 표준을 말한다. 미국의 표준기술연구소(NIST)가 기존의 국가암호 표준인 DES(Data Encryption Standard)를 대체하는 표준으로 AES를 마련키 위해, 암호업계가 제출한 여러 암호 알고리즘에 대해서 시험과정을 거친 후 차세대 국가 암호표준으로 선정하였다.

<14> 이러한 암호화 및 복호화 시스템에서의 안전성은 대개 암호화 키를 관리하는 시스템에 달려있다. 그리고 이러한 암호화 키 관리 시스템에서 가장 중요한 것은 암호화 키를 어떻게 생성하는가 이다.

<15> 암호화 키는 여러가지 정보를 입력받아 생성된다. 입력되는 정보들은 콘텐트 ID, 난수, 그리고 저장장치 ID, 복사 관리 제어 비트(copy management control bits) 등이 있다. 그리고 난수를 어떻게 생성하는가에 따라서 암호화 키가 임의의 값을 갖도록 하는 성질(randomness)이 좋아진다. 난수의 생성방법에 대하여 여러가지 방법이 개시되어 있다. 개시된 여러가지 방법들 중에서는 구현하기가 쉬워 저렴한 비용으로 난수를 생성하는 방법도 있지만, 저렴한 방법을 사용하여 생성된 난수는 의사난수(pseudo-random number)가 되기 때문에 신뢰성이 적다. 즉, 완전한 난수라고는 할 수 없고 아주 긴 주기성을 갖는 난수 형태가 된다. 난수를 몇 비트로 생성하는가에 따라 주기는 길어지므로 난수의 특성(randomness)은 향상된다.

<16> 난수 생성방법의 다른 한가지 방법으로 물리적인 현상을 이용한 난수 생성방법이 있다. 물리적인 현상을 이용한 난수 생성방법은, 장치의 열 잡음(thermal noise)을 이용하여 난수를 생성하는 방법, 하드 디스크에서 발생되는 잡음을 이용하여 난수를 생성하는 방법, 고주파수의 신호를 불안정한 저주파수의 클럭으로 샘플링하여 난수를 생성하는 방법, 역 바이어스 전압을 반도체 실리콘의 p-n 정션(junction)에 인가하여 난수를 생성하는 방법 및 양자역학(quantum mechanics)의 여러가지 현상을 이용하여 난수를 생성하는 방법 등이 있다. 이렇게 물리적인 현상을 이용하면 정확한 난수를 생성할 수 있지만 구현이 복잡하다. 따라서, 특별한 하드웨어적 장치를 필요로 하고 비용도 많이 든다는 문제점이 있다.

【발명이 이루고자 하는 기술적 과제】

<17> 본 발명이 이루고자 하는 기술적 과제는, 오디오 비디오 스트림을 처리하는 시스템이나 오디오 비디오 저장 시스템에서, 입력된 오디오 비디오 스트림을 암호화하는 암호화 장치 및 방법을 제공하는데 있다. 또한 암호화 수행시 사용되는 대칭키를 생성하는데 사용되는 난수 생

성 장치 및 생성방법을 제공하는데 있다. 본 발명에서는, 종래의 난수 생성 알고리즘에 비하여 더 안전하고 저렴하게 구현될 수 있는 난수 생성장치 및 생성방법을 제공한다.

【발명의 구성 및 작용】

<18> 상기의 과제를 이루기 위하여 본 발명에 의한 암호화 장치는, 오디오 비디오 스트림을 입력받아 소정의 처리를 수행하고, 난수 생성에 사용되는 소정의 데이터를 생성하여 출력하는 콘텐트 처리부; 상기 콘텐트 처리부로부터 상기 소정의 데이터를 입력받아 난수를 생성하는 난수 생성부; 상기 난수를 포함하는 정보를 입력받아 암호화키를 생성하는 암호화키 생성부; 및 상기 암호화키를 사용하여 상기 콘텐트 처리부에서 출력된 오디오 비디오 스트림을 암호화하는 콘텐트 암호화부를 구비한다.

<19> 상기의 과제를 이루기 위하여 본 발명에 의한 난수 생성 장치는, 오디오 비디오 스트림을 입력받아 상기 오디오 비디오 스트림의 통계적 특성정보를 생성하여 출력하는 콘텐트 처리부; 및 상기 통계적 특성정보를 입력받아 난수를 생성하는 난수 생성부를 구비한다.

<20> 상기의 과제를 이루기 위하여 본 발명에 의한 암호화 방법은, 오디오 비디오 스트림을 입력받아 소정의 처리를 수행하고, 난수 생성에 사용되는 소정의 데이터를 생성하여 출력하는 단계; 상기 소정의 데이터를 입력받아 난수를 생성하는 단계; 상기 생성된 난수를 포함하는 정보를 입력받아 암호화키를 생성하는 단계; 및 상기 생성된 암호화키를 사용하여 상기 소정의 처리가 수행되어 출력된 오디오 비디오 스트림을 암호화하는 단계를 구비한다.

<21> 상기의 과제를 이루기 위하여 본 발명에 의한 난수 생성 방법은, 오디오 비디오 스트림을 입력받아 상기 오디오 비디오 스트림의 통계적 특성정보를 생성하여 출력하는 단계; 및 상기 통계적 특성정보를 입력받아 난수를 생성하는 단계를 구비한다.

<22> 상기한 과제를 이루기 위하여 본 발명에서는, 상기의 암호화 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

<23> 상기한 과제를 이루기 위하여 본 발명에서는, 상기의 난수 생성 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체를 제공한다.

<24> 이하, 첨부된 도면을 참조하여 본 발명에 따른 바람직한 일실시예를 상세히 설명한다.

<25> 도 1은 오디오 비디오 스트림을 암호화하여 출력하는 장치의 블록도이다.

<26> 오디오 비디오 스트림을 암호화하여 출력하는 장치는 인코딩부(110), 난수 생성부(120), 암호화키 생성부(130) 및 암호화부(140)로 구성되어 있다.

<27> 인코딩부(110)는 오디오 비디오 스트림을 입력받아 인코딩을 수행한다. 인코딩 방법은 MPEG(Moving Picture Expert Group) 표준의 인코딩 방법을 사용한다.

<28> 난수 생성부(120)는 소정의 알고리즘을 이용하여 난수를 생성한다. 난수를 생성하는 알고리즘은 LFSR(Linear Feedback Shift Register)를 사용한 난수 생성 알고리즘, Cellular Automata 알고리즘 등이 있다.

<29> 도 2는 LFSR을 사용한 난수 생성방법을 설명하기 위한 도면이다.

<30> LFSR을 이용한 난수 생성 알고리즘은 소정의 크기의 시프트 레지스터(200)에 초기값을 저장하고, 시프트 레지스터(200)의 특정한 비트(210 내지 240)에 저장된 값들을 부울연산 XOR(Exclusive OR)를 수행하여 새로운 값을 만든다. 도 2의 예에서는 부울연산 '1 XOR 1 XOR 1 XOR 0' 을 수행하게 되므로 만들어진 값은 '1'이 된다. 그리고 시프트 레지스터(200)를 시프트 시키면, 제일 왼쪽 한 비트(250)가 비게 되므로, 부울연산에 의하여 새로 만들어진 값을 시프트 레지스터(200)를 빈 비트(250)에 저장한다. 이렇게 하면 시프트 레지스터(200)에 저장된 값

은 새로운 값이 된다. 시프트 레지스터(200)를 계속해서 한 비트씩 시프트 시키면서 상술한 방법으로 새로운 값을 만들면 난수를 얻을 수 있다. 이렇게 생성된 난수는 엄격히 말하면 정확한 난수는 아닌 의사난수(pseudo random number)이지만 초기값과 특정한 비트(210 내지 240)를 잘 설정하면 좋은 난수 특성을 얻을 수 있다. 특정한 비트의 위치는 임의로 정할 수 있다.

<31> 상술한 LFSR를 사용하여 난수를 생성하는 방법 외에도 물리적인 현상을 이용하여 더 정확하게 난수를 생성하는 방법을 사용할 수도 있고, 두가지 방법들을 조합하여 난수를 생성할 수도 있다.

<32> 암호화키 생성부(130)는 난수 생성부(120)에서 생성된 난수 및 다른 여러가지 정보를 입력받아 암호화키를 생성한다. 다른 여러가지 정보의 예로는, 콘텐트 ID, 저장장치 ID, 복사관리 제어비트 등을 사용할 수 있다. 이러한 정보들을 입력받아 암호화키를 생성하는 방법도 여러가지가 있다. 예를 들어 입력받은 모든 정보에 대하여 부울연산 XOR 하여 생성할 수도 있고, 임의의 비트에 대하여 특정한 부울연산을 수행하여 생성할 수도 있다. 암호화키 생성방법은 암호화키의 특성인 다른 사람이 쉽게 추정할 수 없도록 해야 한다는 점을 고려한다면 어떠한 방법을 사용하여 생성할 수도 있다.

<33> 암호화부(140) 암호화키 생성부(130)에서 생성된 암호화키를 사용하여 인코딩부(110)에서 인코딩된 오디오 비디오 스트림을 입력받아 암호화하여 출력한다.

<34> 도 3은 본 발명의 오디오 비디오 스트림 암호화 장치의 블록도이다.

<35> 콘텐트 처리부(310)는 오디오 비디오 스트림을 입력받아 여러 종류의 처리를 수행한다. 오디오 비디오 스트림을 입력받아 어떠한 처리를 수행하는가에 따라서 난수 생성시에 사용되는 정보가 달라질 수 있다. 즉, 콘텐트 처리부(310)의 원래 기능인 오디오 비디오 스트림의 처리

를 수행하는 동안 그 처리과정에서 부산물로써 생성되는 통계적 특성을 이용하여 난수를 생성하도록 한다. 예를 들어, 이러한 통계적 특성은 매크로 블록의 색 분포(color distribution) 정보, 움직임 추정(motion estimation) 정보, 잡음 추정(noise estimation) 정보 등이 있다. 다시 말하면 콘텐트 처리부(310)는 난수 생성시에 사용될 수 있는 정보를 난수 생성부(320)에 전달하여야 하는데 이러한 정보는 후술하는 여러가지 방법에 의하여 생성될 수 있다.

<36> 그중 한가지 방법은 움직임 추정(Motion Estimation : ME) 모듈에서 생성되는 움직임 벡터(Motion Vector : MV)의 LSB(Least Significant Bit) 1 비트를 사용하는 방법이 있다. 움직임 벡터(MV)는 매크로 블록(macro block)마다 만들어지는데, 매 매크로 블록에서 만들어진 움직임 벡터(MV)의 LSB 1 비트를 소정의 크기의 시프트 레지스터에 순차적으로 저장한다. 만일 128 비트의 시프트 레지스터를 사용한다고 하면, 첫번째 매크로 블록에서 만들어진 움직임 벡터(MV)의 LSB 1 비트를 시프트 레지스터에 저장하고, 시프트 레지스터를 시프트 시킨 후, 다음 매크로 블록에서 만들어진 움직임 벡터(MV)의 LSB 1 비트를 시프트 레지스터에 저장한다. 이러한 방법으로 계속해서 움직임 벡터(MV)의 LSB 1 비트를 저장하면, 시프트 레지스터의 모든 값이 정해진다. 그리고 난수 생성이 필요한 시점에서, 시프트 레지스터에 저장된 값을 난수 생성부(220)로 출력한다.

<37> 다른 방법으로 움직임 추정(ME) 모듈에서의 절대차의 합(Sum of Absolute Difference : SAD) 정보의 LSB 1 비트를 이용하는 방법이 있다. 움직임 벡터(MV)의 LSB 1 비트를 이용하는 것과 동일하게 소정의 크기의 시프트 레지스터에 SAD 정보의 LSB 1 비트를 순차적으로 저장하고 있다가 난수 생성이 필요한 시점에서, 시프트 레지스터에 저장된 값을 난수 생성부(320)로 출력한다.

<38> 또 다른 방법으로 움직임 보상-DCT(Motion Compensation : MC-DCT) 모듈에서 생성된 분산(variance) 정보의 LSB 1 비트를 사용하는 방법이 있다. 상술한 방법들과 동일하게 소정의 크기의 시프트 레지스터에 분산 정보의 LSB 1 비트를 순차적으로 저장하고 있다가 난수 생성이 필요한 시점에서, 시프트 레지스터에 저장된 값을 난수 생성부(320)로 출력한다.

<39> 난수 생성부(320)는 콘텐트 처리부(310)에서 상술한 여러가지 방법에 의해서 생성된 정보를 입력받아 난수를 생성한다. 난수를 생성하는 방법도 여러가지가 있다. 예를 들어 콘텐트 처리부(310)로부터 입력받은 정보를 R 이라고 하고 난수 생성부(320) 자체에서 생성된 난수를 A 라고 하면, 부울연산 'A XOR R' 을 수행한 결과를 난수로 출력할 수 있다. 난수 생성부(320) 자체에서 생성된 난수 A는 종래의 난수 생성 알고리즘인 LFSR를 이용한 난수 생성 알고리즘 또는 Cellular Automata 알고리즘 등을 사용하여 생성될 수 있다.

<40> 암호화키 생성부(330)는 난수 생성부(320)에서 생성된 난수 및 다른 여러가지 정보를 입력받아 암호화키를 생성한다. 다른 여러가지 정보의 예로는, 콘텐트 ID, 저장장치 ID, 복사관리 제어비트 등을 사용할 수 있다. 이러한 정보들을 입력받아 암호화키를 생성하는 방법도 여러가지가 있다. 예를 들어 입력받은 모든 정보에 대하여 부울연산 XOR 하여 생성할 수도 있고, 임의의 비트에 대하여 특정한 부울연산을 수행하여 생성할 수도 있다. 암호화키 생성방법은 암호화키의 특성인 다른 사람이 쉽게 추정할 수 없도록 해야 한다는 점을 고려한다면 어떠한 방법을 사용하여 생성할 수도 있다.

<41> 콘텐트 암호화부(340) 암호화키 생성부(330)에서 생성된 암호화키를 사용하여 콘텐트 처리부(310)에서 출력된 오디오 비디오 스트림을 암호화하여 출력한다.

<42> 도 4는 본 발명의 오디오 비디오 스트림 암호화 방법의 플로우차트이다.

<43> 우선 오디오 비디오 스트림을 입력받아 여러 종류의 처리를 수행한다(S410).

<44> 오디오 비디오 스트림을 입력받아 어떠한 처리를 수행하는가에 따라서 난수 생성시에 사용되는 정보가 달라질 수 있다. 즉, 오디오 비디오 스트림의 처리를 수행하는 동안 그 처리과정에서 부산물로써 생성되는 통계적 특성을 이용하여 난수를 생성한다. 난수 생성에 필요한 정보는 후술하는 방법들에 의하여 생성될 수 있다.

<45> 그중 한가지 방법은 움직임 추정(ME) 모듈에서 생성되는 움직임 벡터(MV)의 LSB 1 비트를 사용하는 방법이 있다. 움직임 벡터(MV)는 매크로 블록(macro block)마다 만들어지는데, 매 매크로 블록에서 만들어진 움직임 벡터(MV)의 LSB 1 비트를 소정의 크기의 시프트 레지스터에 순차적으로 저장한다. 만일 128 비트의 시프트 레지스터를 사용한다고 하면, 첫번째 매크로 블록에서 만들어진 움직임 벡터(MV)의 LSB 1 비트를 시프트 레지스터에 저장하고, 시프트 레지스터를 시프트 시킨 후, 다음 매크로 블록에서 만들어진 움직임 벡터(MV)의 LSB 1 비트를 시프트 레지스터에 저장한다. 이러한 방법으로 계속해서 움직임 벡터(MV)의 LSB 1 비트를 저장하면, 시프트 레지스터의 모든 값이 정해진다. 그리고 난수 생성이 필요한 시점에서, 시프트 레지스터에 저장된 값을 읽어 난수를 생성한다.

<46> 다른 방법으로 움직임 추정(ME) 모듈에서의 절대차의 합(SAD) 정보의 LSB 1 비트를 이용하는 방법이 있다. 움직임 벡터(MV)의 LSB 1 비트를 이용하는 것과 동일하게 소정의 크기의 시프트 레지스터에 SAD 정보의 LSB 1 비트를 순차적으로 저장하고 있다가 난수 생성이 필요한 시점에서, 시프트 레지스터에 저장된 값을 읽어 난수를 생성한다.

<47> 또 다른 방법으로 움직임 보상-DCT(MC-DCT) 모듈에서 생성된 분산(variance) 정보의 LSB 1 비트를 사용하는 방법이 있다. 상술한 방법들과 동일하게 소정의 크기의 시프트 레지스터에

분산 정보의 LSB 1 비트를 순차적으로 저장하고 있다가 난수 생성이 필요한 시점에서, 시프트 레지스터에 저장된 값을 난수를 생성한다.

<48> 난수 생성 단계(S420)는 상술한 여러가지 방법에 의해서 생성된 정보를 입력받아 난수를 생성한다. 난수를 생성하는 방법도 여러가지가 있다. 예를 들어 콘텐트 처리부(310)로부터 입력받은 정보를 R 이라고 하고 난수 생성부(320) 자체에서 생성된 난수를 A 라고 하면, 부울연산 'A XOR R' 을 수행한 결과를 난수로 출력할 수 있다. 난수 생성부(320) 자체에서 생성된 난수 A는 종래의 난수 생성 알고리즘인 LFSR를 이용한 난수 생성 알고리즘 또는 Cellular Automata 알고리즘 등을 사용하여 생성될 수 있다.

<49> 다음으로 암호화키를 생성한다(S430). 난수 생성 단계(S420)에서 생성된 난수 및 다른 여러가지 정보를 입력받아 암호화키를 생성한다. 다른 여러가지 정보의 예로는, 콘텐트 ID, 저장장치 ID, 복사관리 제어비트 등을 사용할 수 있다. 이러한 정보들을 입력받아 암호화키를 생성하는 방법도 여러가지가 있다. 예를 들어 입력받은 모든 정보에 대하여 부울연산 XOR 하여 생성할 수도 있고, 임의의 비트에 대하여 특정한 부울연산을 수행하여 생성할 수도 있다. 암호화키 생성방법은 암호화키의 특성인 다른 사람이 쉽게 추정할 수 없도록 해야 한다는 점을 고려한다면 어떠한 방법을 사용하여 생성할 수도 있다.

<50> 그리고, 암호화키 생성단계(S430)에서 생성된 암호화키를 사용하여 오디오 비디오 스트림을 암호화하여 출력한다(S440).

<51> 본 발명은 또한 컴퓨터로 읽을 수 있는 기록매체에 컴퓨터가 읽을 수 있는 코드로서 구현하는 것이 가능하다. 컴퓨터가 읽을 수 있는 기록매체는 컴퓨터 시스템에 의하여 읽혀질 수 있는 데이터가 저장되는 모든 종류의 기록장치를 포함한다. 컴퓨터가 읽을 수 있는 기록매체의 예로는 ROM, RAM, CD-ROM, 자기 테이프, 플로피디스크, 광 데이터 저장장치 등이 있으며,

또한 캐리어 웨이브(예를 들어 인터넷을 통한 전송)의 형태로 구현되는 것도 포함한다. 또한 컴퓨터가 읽을 수 있는 기록매체는 네트워크로 연결된 컴퓨터 시스템에 분산되어, 분산방식으로 컴퓨터가 읽을 수 있는 코드가 저장되고 실행될 수 있다.

<52> 이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

【발명의 효과】

<53> 상술한 바와 같이 본 발명은, 생성된 난수의 랜덤 특성(randomness)이 좋은 효과가 있다. 그 이유는 일반적으로 비디오 데이터 자체는 시간적으로나 공간적으로 랜덤한 특성을 가지고 있고, 이 랜덤한 정보를 이용하여 난수를 생성하였기 때문이다. 따라서 생성된 키는 다른 정보와 연관성(correlation)이 적고, 예측 가능하지 않으므로 안전성을 높일 수 있는 효과가 있다.

<54> 또한, 난수는 각각의 오디오 비디오 스트림을 이용하여 생성되기 때문에, 입력된 오디오 비디오 스트림이 다른 경우에는 생성된 암호화키도 다르다. 따라서 시스템을 공격하는 공격자가 암호화키 생성부를 해킹하는데 성공하였다고 하더라도 더 안전하다. 따라서 암호화키 생성부의 내부 알고리즘을 알고 있다고 하더라도, 암호화키는 콘텐트 처리부에서 생성되는 정보에 의해서 생성되기 때문에 복호화할 수 없다. 따라서 암호화키 생성부에 있는 의사난수 생성부를 파악할 수 있다고 하더라도 암호화된 오디오 비디오 스트림을 복호화하는데 충분하지 않다.

<55> 그리고, 본 발명은 기본적으로 알고리즘에 기반을 두기 때문에 비용이 적게 든다. 즉, 난수를 생성하기 위하여 특별한 하드웨어 장치를 필요로 하지 않고 상술한 방법을 구현하는 소프트웨어나 하드웨어 어느 것이든 사용될 수 있다.

【특허청구범위】

【청구항 1】

오디오 비디오 스트림을 입력받아 소정의 처리를 수행하고, 난수 생성에 사용되는 소정의 데이터를 생성하여 출력하는 콘텐트 처리부;

상기 콘텐트 처리부로부터 상기 소정의 데이터를 입력받아 난수를 생성하는 난수 생성부;

상기 난수를 포함하는 정보를 입력받아 암호화키를 생성하는 암호화키 생성부; 및

상기 암호화키를 사용하여 상기 콘텐트 처리부에서 출력된 오디오 비디오 스트림을 암호화하는 콘텐트 암호화부를 포함하는 것을 특징으로 하는 암호화 장치.

【청구항 2】

제1항에 있어서, 상기 콘텐트 처리부에서 수행되는 소정의 처리는

상기 오디오 비디오 스트림을 입력받아 수행되는 MPEG 비디오 압축 처리인 것을 특징으로 하는 암호화 장치.

【청구항 3】

제1항에 있어서, 상기 콘텐트 처리부에서 생성되는 소정의 데이터는

상기 오디오 비디오 스트림을 입력받아 MPEG 비디오 압축 처리를 수행하면서 상기 오디오 비디오 스트림의 통계적 특성을 기초로 생성되는 데이터인 것을 특징으로 하는 암호화 장치.

【청구항 4】

제3항에 있어서, 상기 통계적 특성은

상기 오디오 비디오 스트림에 대하여 수행되는 MPEG 비디오 압축 처리과정에서 생성되는 매크로 블록의 색 분포 정보 또는 움직임 추정 정보 또는 잡음 추정 정보인 것을 특징으로 하는 암호화 장치.

【청구항 5】

제1항에 있어서, 상기 콘텐트 처리부는

움직임 추정(ME) 과정에서 생성되는 움직임 벡터(MV) 정보를 기초로 난수 생성에 사용되는 소정의 데이터를 생성하여 출력하는 것을 특징으로 하는 암호화 장치.

【청구항 6】

제5항에 있어서, 상기 소정의 데이터는

움직임 추정(ME) 과정에서 생성되는, 매크로 블록에 대한 움직임 벡터(MV)의 LSB 1 비트가 시프트 레지스터에 저장되고, 상기 시프트 레지스터를 한 비트씩 시프트 시키면서 다음 매크로 블록의 움직임 벡터(MV)의 LSB 1 비트가 순차적으로 저장되어 있다가 난수 생성 요청시에 저장되어 있는 상태의 시프트 레지스터 값인 것을 특징으로 하는 암호화 장치.

【청구항 7】

제1항에 있어서, 상기 콘텐트 처리부는

움직임 추정(ME) 과정에서 생성되는 절대차의 합(SAD) 정보를 기초로 난수 생성에 사용되는 소정의 데이터를 생성하여 출력하는 것을 특징으로 하는 암호화 장치.

【청구항 8】

제7항에 있어서, 상기 소정의 데이터는

움직임 추정(ME) 과정에서 생성되는, 매크로 블록에 대한 절대차의 합(SAD) 정보의 LSB 1 비트가 시프트 레지스터에 저장되고, 상기 시프트 레지스터를 한 비트씩 시프트 시키면서 다음 매크로 블록의 절대차의 합(SAD) 정보의 LSB 1 비트가 순차적으로 저장되어 있다가 난수 생성 요청시에 저장되어 있는 상태의 시프트 레지스터 값인 것을 특징으로 하는 암호화 장치.

【청구항 9】

제1항에 있어서, 상기 콘텐트 처리부는

움직임 보상-DCT(MC-DCT) 과정에서 생성된 분산(variance) 정보를 기초로 난수 생성에 사용되는 소정의 데이터를 생성하여 출력하는 것을 특징으로 하는 암호화 장치.

【청구항 10】

제9항에 있어서, 상기 소정의 데이터는

움직임 보상-DCT(MC-DCT) 과정에서 생성된 분산(variance) 정보의 LSB 1 비트가 시프트 레지스터에 저장되고, 상기 시프트 레지스터를 한 비트씩 시프트 시키면서 다음 분산(variance) 정보의 LSB 1 비트가 순차적으로 저장되어 있다가 난수 생성 요청시에 저장되어 있는 상태의 시프트 레지스터 값인 것을 특징으로 하는 암호화 장치.

【청구항 11】

제1항에 있어서, 상기 난수 생성부는

상기 콘텐트 처리부로부터 전달받은 소정의 데이터와 상기 난수 생성부 자체에서 소정의 알고리즘에 의하여 생성된 난수에 대하여 소정의 연산을 수행하여 난수를 생성하는 것을 특징으로 하는 암호화 장치.

【청구항 12】

제11항에 있어서, 상기 소정의 연산은

XOR 부울연산인 것을 특징으로 하는 암호화 장치.

【청구항 13】

제11항 또는 제12항에 있어서, 상기 소정의 알고리즘은

LFSR(Linear Feedback Shift Register)를 이용한 난수 생성 알고리즘 또는 Cellular Automata 알고리즘인 것을 특징으로 하는 암호화 장치.

【청구항 14】

제1항에 있어서, 상기 암호화키 생성부는

상기 난수 생성부에서 생성된 난수 및 콘텐트 ID 정보, 저장장치 ID 정보, 복사관리 제어비트정보를 더 입력받아 소정의 연산을 수행하여 암호화키를 생성하는 것을 특징으로 하는 암호화 장치.

【청구항 15】

제14항에 있어서, 상기 소정의 연산은

상기 입력받은 모든 정보에 대한 XOR 부울연산 이거나 또는 상기 입력받은 모든 정보의 소정의 임의의 비트에 대한 XOR 부울연산인 것을 특징으로 하는 암호화 장치.

【청구항 16】

오디오 비디오 스트림을 입력받아 상기 오디오 비디오 스트림의 통계적 특성정보를 생성하여 출력하는 콘텐트 처리부; 및

상기 통계적 특성정보를 입력받아 난수를 생성하는 난수 생성부를 포함하는 것을 특징으로 하는 난수 생성 장치.

【청구항 17】

제16항에 있어서, 상기 통계적 특성정보는

움직임 추정(ME) 과정에서 생성되는 움직임 벡터(MV) 정보 또는 움직임 추정(ME) 과정에서 생성되는 절대차의 합(SAD) 정보 또는 움직임 보상-DCT(MC-DCT) 과정에서 생성된 분산(variance) 정보인 것을 특징으로 하는 난수 생성 장치.

【청구항 18】

제16항에 있어서, 상기 통계적 특성정보는

움직임 추정(ME) 과정에서 생성되는, 매크로 블록에 대한 움직임 벡터(MV)의 LSB 1 비트가 시프트 레지스터에 저장되고, 상기 시프트 레지스터를 한 비트씩 시프트 시키면서 다음 매크로 블록의 움직임 벡터(MV)의 LSB 1 비트가 순차적으로 저장되어 있다가 난수 생성 요청시에 저장되어 있는 상태의 시프트 레지스터 값인 것을 특징으로 하는 난수 생성 장치.

【청구항 19】

제16항에 있어서, 상기 통계적 특성정보는

움직임 추정(ME) 과정에서 생성되는, 매크로 블록에 대한 절대차의 합(SAD) 정보의 LSB 1 비트가 시프트 레지스터에 저장되고, 상기 시프트 레지스터를 한 비트씩 시프트 시키면서 다음 매크로 블록의 절대차의 합(SAD) 정보의 LSB 1 비트가 순차적으로 저장되어 있다가 난수 생성 요청시에 저장되어 있는 상태의 시프트 레지스터 값인 것을 특징으로 하는 난수 생성 장치.

【청구항 20】

제16항에 있어서, 상기 통계적 특성정보는

움직임 보상-DCT(MC-DCT) 과정에서 생성된 분산(variance) 정보의 LSB 1 비트가 시프트 레지스터에 저장되고, 상기 시프트 레지스터를 한 비트씩 시프트 시키면서 다음 분산(variance) 정보의 LSB 1 비트가 순차적으로 저장되어 있다가 난수 생성 요청시에 저장되어 있는 상태의 시프트 레지스터 값인 것을 특징으로 하는 난수 생성 장치.

【청구항 21】

(a) 오디오 비디오 스트림을 입력받아 소정의 처리를 수행하고, 난수 생성에 사용되는 소정의 데이터를 생성하여 출력하는 단계;

(b) 상기 소정의 데이터를 입력받아 난수를 생성하는 단계;

(c) 상기 생성된 난수를 포함하는 정보를 입력받아 암호화키를 생성하는 단계; 및

(d) 상기 생성된 암호화키를 사용하여 상기 소정의 처리가 수행되어 출력된 오디오 비디오 스트림을 암호화하는 단계를 포함하는 것을 특징으로 하는 암호화 방법.

【청구항 22】

제21항에 있어서, 상기 (a) 단계에서 수행되는 소정의 처리는

상기 오디오 비디오 스트림을 입력받아 수행되는 MPEG 비디오 압축 처리인 것을 특징으로 하는 암호화 방법.

【청구항 23】

제21항에 있어서, 상기 (a) 단계에서 생성되는 소정의 데이터는

상기 오디오 비디오 스트림을 입력받아 MPEG 비디오 압축 과정을 수행하면서 상기 오디오 비디오 스트림의 통계적 특성인 매크로 블록의 색 분포 정보 또는 움직임 추정 정보 또는 잡음 추정 정보를 기초로 생성되는 데이터인 것을 특징으로 하는 암호화 방법.

【청구항 24】

제21항에 있어서, 상기 (a) 단계는

움직임 추정(ME) 과정에서 생성되는 움직임 벡터(MV) 정보 또는 움직임 추정(ME) 과정에서 생성되는 절대차의 합(SAD) 정보 또는 움직임 보상-DCT(MC-DCT) 과정에서 생성된 분산(variance) 정보를 기초로 난수 생성에 사용되는 소정의 데이터를 생성하여 출력하는 것을 특징으로 하는 암호화 방법.

【청구항 25】

제21항에 있어서, 상기 (a) 단계는

움직임 추정(ME) 과정에서 매 매크로 블록마다 생성되는 움직임 벡터(MV)의 LSB 1 비트 또는 움직임 추정(ME) 과정에서 생성되는 절대차의 합(SAD) 정보의 LSB 1 비트 또는 움직임 보상-DCT(MC-DCT) 과정에서 생성된 분산(variance) 정보의 LSB 1 비트를 소정의 크기의 시프트 레지스터에 시프트 레지스터를 시프트 시키면서 순차적으로 저장하고 난수 생성 요청이 입력되면 상기 시프트 레지스터에 저장된 값을 출력하는 것을 특징으로 하는 암호화 방법.

【청구항 26】

제21항에 있어서, 상기 (b) 단계는

상기 (a) 단계에서 전달받은 소정의 데이터와 소정의 난수 생성 알고리즘에 의하여 생성된 난수에 대하여 소정의 연산을 수행하여 난수를 생성하는 것을 특징으로 하는 암호화 방법.

【청구항 27】

제26항에 있어서, 상기 소정의 난수 생성 알고리즘은

LFSR(Linear Feedback Shift Register)를 이용한 난수 생성 알고리즘 또는 Cellular Automata 알고리즘인 것을 특징으로 하는 암호화 방법.

【청구항 28】

제21항에 있어서, 상기 (c) 단계는

상기 (b) 단계에서 생성된 난수 및 콘텐트 ID 정보, 저장장치 ID 정보, 복사관리 제어비트정보를 더 입력받아 소정의 연산을 수행하여 암호화 키를 생성하는 것을 특징으로 하는 암호화 방법.

【청구항 29】

제28항에 있어서, 상기 소정의 연산은

상기 입력받은 모든 정보에 대한 XOR 부울연산 이거나 또는 상기 입력받은 모든 정보의 소정의 임의의 비트에 대한 XOR 부울연산인 것을 특징으로 하는 암호화 방법.

【청구항 30】

(a) 오디오 비디오 스트림을 입력받아 상기 오디오 비디오 스트림의 통계적 특성정보를 생성하여 출력하는 단계; 및

(b) 상기 통계적 특성정보를 입력받아 난수를 생성하는 단계를 포함하는 것을 특징으로 하는 난수 생성 방법.

【청구항 31】

제30항에 있어서, 상기 통계적 특성정보는

움직임 추정(ME) 과정에서 생성되는 움직임 벡터(MV) 정보 또는 움직임 추정(ME) 과정에서 생성되는 절대차의 합(SAD) 정보 또는 움직임 보상-DCT(MC-DCT) 과정에서 생성된 분산(variance) 정보인 것을 특징으로 하는 난수 생성 방법.

【청구항 32】

제30항에 있어서, 상기 통계적 특성정보는

움직임 추정(ME) 과정에서 생성되는, 매크로 블록에 대한 움직임 벡터(MV)의 LSB 1 비트가 시프트 레지스터에 저장되고, 상기 시프트 레지스터를 한 비트씩 시프트 시키면서 다음 매크로 블록의 움직임 벡터(MV)의 LSB 1 비트가 순차적으로 저장되어 있다가 난수 생성 요청시에 저장되어 있는 상태의 시프트 레지스터 값인 것을 특징으로 하는 난수 생성 방법.

【청구항 33】

제30항에 있어서, 상기 통계적 특성정보는

움직임 추정(ME) 과정에서 생성되는, 매크로 블록에 대한 절대차의 합(SAD) 정보의 LSB 1 비트가 시프트 레지스터에 저장되고, 상기 시프트 레지스터를 한 비트씩 시프트 시키면서 다음 매크로 블록의 절대차의 합(SAD) 정보의 LSB 1 비트가 순차적으로 저장되어 있다가 난수 생성 요청시에 저장되어 있는 상태의 시프트 레지스터 값인 것을 특징으로 하는 난수 생성 방법.

【청구항 34】

제30항에 있어서, 상기 통계적 특성정보는

움직임 보상-DCT(MC-DCT) 과정에서 생성된 분산(variance) 정보의 LSB 1 비트가 시프트 레지스터에 저장되고, 상기 시프트 레지스터를 한 비트씩 시프트 시키면서 다음 분산

(variance) 정보의 LSB 1 비트가 순차적으로 저장되어 있다가 난수 생성 요청시에 저장되어 있는 상태의 시프트 레지스터 값인 것을 특징으로 하는 난수 생성 방법.

【청구항 35】

(a) 오디오 비디오 스트림을 입력받아 소정의 처리를 수행하고, 난수 생성에 사용되는 소정의 데이터를 생성하여 출력하는 단계;

(b) 상기 소정의 데이터를 입력받아 난수를 생성하는 단계;

(c) 상기 생성된 난수를 포함하는 정보를 입력받아 암호화키를 생성하는 단계; 및

(d) 상기 생성된 암호화키를 사용하여 상기 소정의 처리가 수행되어 출력된 오디오 비디오 스트림을 암호화하는 단계를 포함하는 것을 특징으로 하는 암호화 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

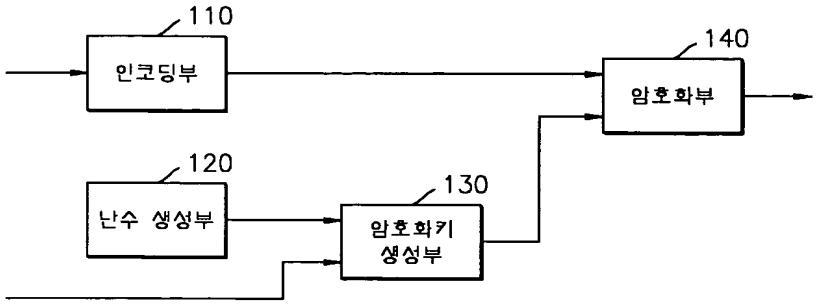
【청구항 36】

(a) 오디오 비디오 스트림을 입력받아 상기 오디오 비디오 스트림의 통계적 특성정보를 생성하여 출력하는 단계; 및

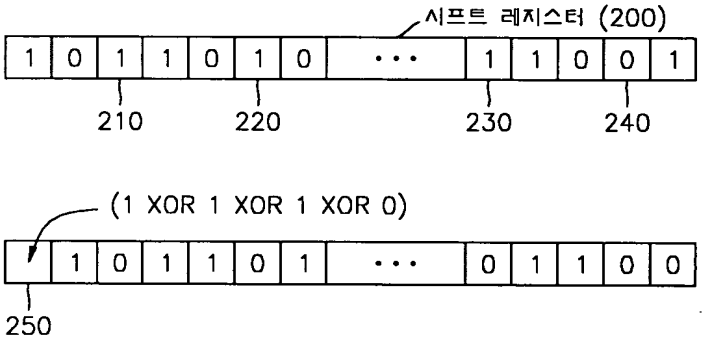
(b) 상기 통계적 특성정보를 입력받아 난수를 생성하는 단계를 포함하는 것을 특징으로 하는 난수 생성 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

【도면】

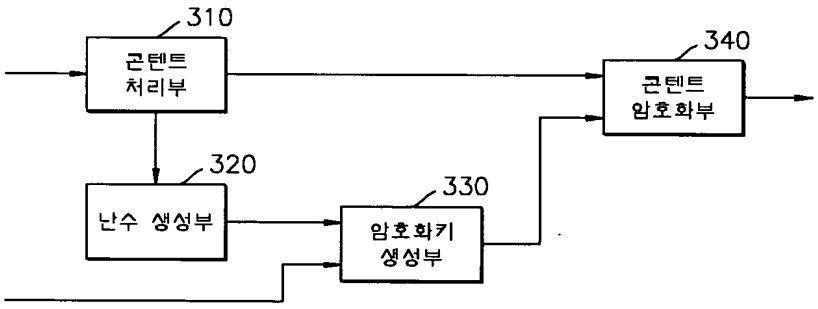
【도 1】


110
인코딩부
140
암호화부
120
난수 생성부
130
암호화키
생성부

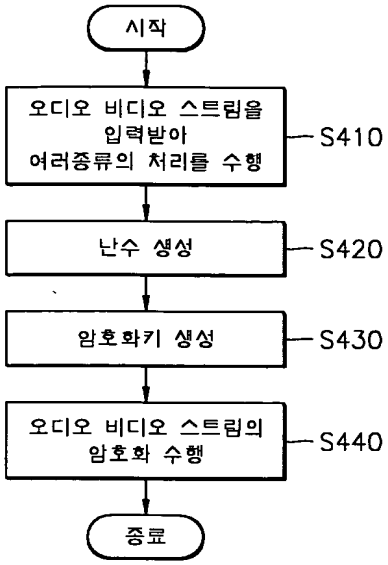
【도 2】


시프트 레지스터 (200)
1 0 1 1 0 1 0 • • • 1 1 0 0 1
210
220
230
240
(1 XOR 1 XOR 1 XOR 0)
1 1 0 1 1 0 1 • • • 0 1 1 0 0
250

【도 3】


310
콘텐트
처리부
340
콘텐트
암호화부
320
난수 생성부
330
암호화키
생성부

【도 4】


시작
오디오 비디오 스트림을 입력받아 여러종류의 처리를 수행
S410
난수 생성
S420
암호화키 생성
S430
오디오 비디오 스트림의 암호화 수행
S440
종료